Méthodes d'enquête pénales et protection des personnes vulnérables dans l'environnement numérique

Forget, Catherine

Published in:
Vulnérabilités et droits dans l'environnement numérique

Publication date:
2018

Document Version
le PDF de l'éditeur

Chapitre 6
Méthodes d'enquête pénales et protection des personnes vulnérables dans l'environnement numérique

Catherine Forget[1]

Introduction

Dans le cadre de l'enquête pénale, la personne « vulnérable » n'est pas forcément le témoin ou la victime d'une infraction pénale. Indépendamment de son statut dans le cadre du procès pénal, le législateur offre des garanties particulières à certaines personnes ou catégories de personnes susceptibles de connaitre une ingérence dans leurs droits fondamentaux. En effet, dans l'environnement numérique, les méthodes d'enquête entraînent essentiellement une atteinte dans le droit au respect de la vie privée et le droit à la protection des données à caractère personnel garantis par l'article 22 de la Constitution, l'article 8 de la Convention européenne des droits de l'homme (ci-après « la CEDH »)[2] et les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne (ci-après « la Charte »)[3]. Si le choix entre les différentes techniques d'enquête relève essentiellement du pouvoir discrétionnaire des États, ceux-ci ne dis-

[1] Avocate au barreau de Bruxelles et chercheuse au CRIDS (Université de Namur).

[2] L'article 8, § 1, de la CEDH au terme d'une jurisprudence abondante, garantit le droit à la protection des données à caractère personnel mais aussi, sous le couvert du droit à la correspondance, le droit à la confidentialité des communications électroniques. Voy. Cour eur. D.H., *Copland c. Royaume-Uni*, 3 avril 2007, n° 62617/00. En effet, dans l'interprétation de l'article 8 de la CEDH, est prise en compte la Convention 108 du Conseil de l'Europe, seul instrument contraignant en matière de protection de données au niveau mondial (Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STCE n° 108, 1981). Voy. Cour eur. D.H., *Amann c. Suisse,* 4 mai 2000, n° 27798/5, § 65.

[3] La Charte distingue expressément les deux dispositions encadrant dès lors tout traitement de données à caractère personnel indépendamment d'une atteinte éventuelle à la vie privée (C. Docksey, « Articles 7 and 8 of the EU Charter : two distinct fundamental rights », in *Quelle protection des données personnelles en Europe ?*, Bruxelles, Larcier, 2015, pp. 71-97).

posent pas pour autant, d'une latitude illimitée[4]. En vertu des articles 8, § 2, de la CEDH et 52, § 1, de la Charte, la procédure applicable doit s'inscrire dans le respect des critères de légalité, de nécessité et de proportionnalité en vue de prémunir la personne concernée contre les risques d'ingérences illicites ou arbitraires des pouvoirs publics.

En droit national belge, la phase préliminaire de la procédure pénale belge est dite « inquisitoire » c'est-à-dire secrète, unilatérale et écrite[5]. En principe, seul le juge d'instruction est habilité à poser un acte de contrainte susceptible de porter atteinte aux droits et libertés individuelles[6]. En effet, celui-ci instruit à charge et à décharge de manière « indépendante et impartiale » alors que le procureur du Roi assume « le rôle de la partie poursuivante » dans le cadre de l'information[7] et « ne peut donc être considéré comme impartial »[8]. Cette répartition des rôles semble toutefois s'assouplir au fil du temps compte tenu de la multiplication des exceptions permettant au procureur du Roi d'agir dans des matières réservées au juge d'instruction par exemple, en cas de flagrant délit[9] ou dans les conditions prévues par la mini-instruction[10]. De plus, depuis l'adoption de la loi du 6 janvier 2003[11], le procureur du Roi peut procéder à des méthodes particulières de recherche telles l'observation, l'infiltration et le recours aux indicateurs, méthodes considérées comme particulièrement invasives pour les droits et libertés fondamentales[12]. La loi du 25 décembre

[4] Cour eur. D.H., *Gerhard Klass e.a. c. Allemagne*, 6 septembre 1978, n° 5029/71, § 49.

[5] A. Jacobs, « Petit tour du monde du contradictoire », in C. Ribeyre (dir.), *Le contradictoire dans le procès pénal : nouvelles perspectives*, Cujas, Paris, 2012, p. 26.

[6] Art. 28, § 3, CICr.

[7] Art. 28*bis* CICr.

[8] C. const., 25 janvier 2017, arrêt n° 6/2017, C 6325 et 6326, B.5.2.

[9] À titre illustratif, en cas de flagrant délit (ou de situation assimilées), le procureur du Roi peut ouvrir un courrier postal (art. 46*ter* CICr), il peut procéder à une visite domiciliaire dans le domicile de l'inculpé (art. 36 CICr), il peut dans certain cas ordonner le repérage et la localisation des communications (art. 88*bis* CICr).

[10] La mini-instruction réglementée par l'article 28*septies* CICr permet au procureur du Roi de requérir du juge d'instruction l'accomplissement d'un acte d'instruction sans pour autant réellement ouvrir une instruction. Certains actes restent néanmoins de la compétence unique du juge d'instruction notamment l'interception des communications et l'observation avec des moyens techniques dans un domicile visés respectivement par les articles 90*ter* et 89*ter* CICr en raison de l'ingérence particulièrement importante pour les droits et libertés des personnes.

[11] Loi du 6 janvier 2003 concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête, *M.B.*, 12 mai 2003.

[12] Elles sont particulières dans le sens où elles sont susceptibles de porter atteinte aux libertés et droits fondamentaux. De plus, à la différence des autres méthodes d'enquêtes, les enquêteurs établissent un dossier confidentiel où sont glissées certaines pièces du dossier (*Doc. parl.*, Ch. repr., 2001-2002, n° 50-1688/001, p. 132).

2016 s'inscrit dans cette même dynamique, celle-ci offrant des nouvelles méthodes aux enquêteurs ou clarifiant le cadre légal préexistant tout en laissant transparaître un accroissement des compétences du procureur du Roi[13] à l'heure où la place et le rôle du magistrat instructeur font l'objet de vives discussions[14].

Dans le cadre de cette contribution, nous exposerons successivement les mesures mises en place dans un contexte informatique et les différentes protections accordées par le législateur à certaines catégories de personnes telles que : l'hébergeur, les personnes actives sur Internet, les personnes soumises au secret professionnel, les usagers de services de communications électroniques, le tiers à l'enquête pénale et le suspect dans le cadre de l'obligation de collaboration. Nous verrons que l'exercice entre souci d'efficacité et respect des droits fondamentaux peut s'avérer périlleux.

SECTION 1. – L'exonération de responsabilité de l'hébergeur

Sur Internet, le blocage rapide de contenu « manifestement illicite » de type révisionniste, pédophile ou encore incontestablement outrageant peut s'avérer une véritable gageure pour les autorités. En conséquence, les prestataires intermédiaires de l'Internet[15] sont tenus de dénoncer « sans délai » aux autorités, les activités ou informations illicites alléguées

[13] Loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales, *M.B.,* 17 janvier 2017. Pour un commentaire sur la loi du 25 décembre 2016, voy. C. Conings et S. Royer, « Verzamelen en vastleggen van digitaal bewijs in strafzaken », *N.C.,* 2017/4, pp. 313-320 ; V. Franssen et S. Tosza, « Vers plus de droits pour le justiciable sur internet ? Un nouveau cadre légal pour lutter contre la criminalité dans la société de l'information », in *Les droits des justiciables face à la justice pénale,* Limal, Anthemis, 2017, pp. 205-249 ; C. Forget, « Les nouvelles méthodes d'enquête dans un contexte informatique, vers un cadre (plus) strict ? », *R.D.T.I.,* 2017, n° 66-67, pp. 25-52.

[14] À ce propos, voy. M.-A. Beernaert, « Du juge d'instruction au juge de l'enquête : raisons et contours de la réforme proposée », in *La figure du juge d'instruction : réformer ou supprimer ?*, Bruxelles, Larcier, 2017, pp. 21-28 ; L. Kennes et D. Scalia, *Du juge d'instruction vers le juge de l'enquête : analyse critique et de droit comparé,* Bruxelles, Anthemis, 2017.

[15] Il s'agit des fournisseurs d'infrastructures, les fournisseurs d'accès et les fournisseurs des services types réseaux sociaux, moteurs de recherche, les services de 'cloud' et autres activités d'hébergement. À ce propos, voy. F. Jongen et A. Strowel, *Droit des médias et de la communication*, Bruxelles, Larcier, 2017, p. 782.

qu'exerceraient les destinataires de leurs services[16]. Cette obligation ne pourrait toutefois se généraliser en leur imposant de mettre en place un système de filtrage par exemple[17] et ce, afin de préserver le droit à la liberté d'expression[18]. De plus, comme le relève la Cour de justice de l'Union européenne dans le cadre de l'affaire *Scarlet*, obliger un intermédiaire à mettre en place un système informatique complexe, coûteux, permanent et à ses seuls frais et ce, afin de prévenir les téléchargements illégaux, engendrerait une atteinte disproportionnée à la liberté d'entreprise, un droit fondamental pour les opérateurs économiques[19].

L'hébergeur[20] a davantage de responsabilités que tout autre intermédiaire puisqu'après avoir communiqué « sur le champ » au procureur du Roi les activités ou informations illicites, dont il aurait effectivement connaissance[21], celui-ci doit prendre des mesures pour empêcher l'accès aux données[22]. En contrepartie, il ne peut être tenu pour responsable des informations stockées par un destinataire de ses services à la condition de ne pas en avoir eu connaissance *effective*[23]. Cette exonération de responsabilité vise uniquement l'hébergeur dans la mesure où son rôle se limite à « celui d'un prestataire passif de services purement techniques » à la différence de l'éditeur de contenu par exemple[24]. En ce sens, la Cour de justice

[16] Art. XII. 17 et s. CDE. Ces dispositions transposent la directive 2000/13 sur le commerce électronique. Voy. directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, *O.J.*, L 178, 17 juillet 2000, pp. 1-16.

[17] C.J.U.E., 24 novembre 2011, *Scarlet Extended SA / SABAM,* C-70/10.

[18] Art. XII. 18 CDE. À cet égard voy. : E. Montero et Q. Van Enis, « Ménager la liberté d'expression au regard des mesures de filtrage imposées aux intermédiaires de l'internet : la quadrature du cercle ? », *R.L.D.I.,* 2010, pp. 88-89. Par contre, dans certaines situations prévues par la loi, les intermédiaires peuvent être tenus de surveiller temporairement et spécifiquement les destinataires de leurs services. Art. XII. 20, § 2, du Code de droit économique ; S. Dussolier, « Responsabilités des intermédiaires de l'Internet : un équilibre compromis ? », *R.D.T.I.*, 2007/29, p. 271.

[19] C.J.U.E., 24 novembre 2011, *Scarlet Extended SA / SABAM*, C-70/10.

[20] Selon le Code de droit économique, l'hébergeur est celui qui fournit un « service de la société de l'information consistant à stocker des informations fournies par un destinataire du service ». Art. XII. 19, § 1, CDE.

[21] Art. XII. 19, § 1, 2°, CDE.

[22] Art. XII.19, § 3, CDE. Pour un approfondissement sur la notion d'hébergement voy. E. Montero, « Commerces électroniques et contrats de l'informatique », *Chronique de jurisprudence en droit des technologies de l'information (2009-2011)*, *R.D.T.I.*, 2012/4849, pp. 22 et s.

[23] Art. XII. 17 et 18 CDE.

[24] Il n'est pas toujours aisé de déterminer quels acteurs bénéficient de cette exonération de responsabilité, la limite entre éditeur de contenu et hébergeur étant parfois ténue. Ainsi, dans l'affaire *Delfi c. Estonie*, la Cour européenne des droits de l'homme a considéré

de l'Union européenne a qualifié d'hébergeur la société dont le rôle exercé est « neutre, en ce que son comportement est purement technique, automatique et passif, impliquant l'absence de connaissance ou de contrôle des données qu'il stocke »[25]. Pour bénéficier de l'exonération de responsabilité, le prestataire ne doit donc jouer aucun rôle actif de nature à lui permettre de prendre connaissance ou à contrôler les données stockées[26]. Il doit, pour le surplus, avoir agi *promptement* pour retirer les informations ou rendre l'accès à celles-ci impossible dès la prise de connaissance[27].

SECTION 2. – Les personnes actives sur Internet

Sur Internet, des images pédopornographiques s'échangent avec une facilité déconcertante par le biais de réseau de partage de fichier (*peer-to-peer*) où les utilisateurs agissent à la fois en tant que « client » et « serveur » en mettant à disposition les fichiers téléchargés et en les partageant.

---

qu'une société commerciale gestionnaire d'un site web invitant les internautes à déposer des commentaires et à réagir aux articles de presse publiés sur son site, ne pouvait bénéficier de l'exonération de responsabilité des hébergeurs. Selon la Cour, le rôle joué par la société dépassait « celui d'un prestataire passif de services purement techniques » notamment en ce qu'elle retirait d'elle-même les messages qui lui semblaient illicites sans attendre une éventuelle notification d'une personne s'estimant lésée de sorte qu'elle aurait dû prendre des mesures pour retirer les commentaires injurieux dans les meilleurs délais après leur publication (Cour eur. D.H., *Delfi AS c. Estonie*, 16 juin 2015, n° 64569/09. Pour un commentaire voy. E. Montero et Q. Van Enis, « Les gestionnaires de forums et portails d'actualités cueillis à froid par la Cour de Strasbourg ? : (obs. sous Cour eur. dr. h., Gde Ch., arrêt Delfi AS c. Estonie, 16 juin 2015) », *Rev. trim. D.H.*, 2016/9, pp. 953-981).

[25] C.J.U.E., 23 mars 2010, *Google France c. Google*, aff. jointes, C-236/08, C-237/08 et C-238/08, §§ 112 et 113.

[26] Notons qu'une proposition de directive du Parlement européen et du Conseil sur le droit d'auteur prévoit de renverser ce système en imposant aux prestataires de services de la société de l'information qui stockent un grand nombre d'œuvres et qui donnent accès à ces œuvres et autres objets de prendre des mesures visant *a priori*, à protéger les droits d'auteurs. À cette fin, les prestataires de services devraient prévoir des techniques efficaces de reconnaissance des contenus. Voy. art. 13, § 1, de la Proposition de directive du Parlement européen et du Conseil sur le droit d'auteur dans le marché unique numérique, Bruxelles, 14 septembre 2016, COM(2016) 593 final.

[27] Art. XII. 19, § 1, 1°, CDE. La loi ne précise pas si le critère à prendre en considération est le moment de la connaissance de l'existence d'une infraction ou le moment de la connaissance de l'activité illicite (F. Jongen et A. Strowel, *Droit des médias et de la communication*, *op. cit.*, p. 787) via par exemple, une procédure « *notice and take down* » ou « notification et action ». La mise en place de ce type de procédure est recommandée par l'Union européenne afin de faciliter le blocage de site Internet. Voy. Recommandation (UE) 2018/334 de la Commission du 1er mars 2018 sur les mesures destinées à lutter, de manière efficace, contre les contenus illicites en ligne, *J.O.*, L 63, 6 mars 2018, pp. 50-61.

Pour obtenir l'identité des personnes actives sur ces réseaux, les autorités peuvent adresser une demande aux fournisseurs d'accès Internet. Cette demande ne peut toutefois se faire sans prévoir un cadre légal adéquat[28]. En ce sens, la Cour européenne des droits de l'homme a rappelé que la communication relative à l'identité des utilisateurs « nécessite généralement une injonction des autorités d'enquête ou des autorités judiciaires, et elle est soumise à des conditions restrictives »[29].

En ce sens, le Code d'instruction criminelle permet au procureur du Roi de solliciter le concours des opérateurs et fournisseurs de communications électroniques tels Base, Orange, Proximus mais aussi les services dits « *over the top* » tels WhatsApp, Viber, Facebook ou encore Skype[30] afin de procéder à l'identification d'un utilisateur de ses services en obtenant par exemple, selon le cas, les informations relatives à une ligne téléphonique, une adresse de courrier électronique, une adresse IP, un code 'IMEI' d'un téléphone[31], l'adresse 'MAC' d'un ordinateur[32]. Dans le cas où l'infraction n'est pas de nature à emporter une peine d'emprisonnement correctionnel principal d'un an ou une peine plus lourde[33], le procureur du Roi ne peut requérir que les données d'indentification conservées depuis six mois à partir de sa décision[34].

---

[28] Cour eur. D.H., *Benedik c. Slovénie,* 24 avril 2018, n° 62357/14.

[29] Cour eur. D.H., *Delfi AS c. Estonie*, 16 juin 2015, n° 64569/09, § 148.

[30] La jurisprudence *Yahoo* entérinée par la loi du 25 décembre 2016 élargit le spectre des tiers tenus de collaborer dans le cadre des méthodes d'enquêtes relatives au communications électroniques à savoir, l'identification, le repérage ou l'interception des communications. Ces mesures ne concernent plus uniquement les « opérateurs de réseaux de communications électroniques » traditionnels mais visent de manière plus générale la coopération de « toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques » en ce inclus « le fournisseur d'un service de communications électroniques ». Voy. not. : C. Forget, « Les nouvelles méthodes d'enquête dans un contexte informatique, vers un cadre (plus) strict ? », *op. cit.*, pp. 25-52.

[31] International Mobile Equipment Identity. L'IMEI est un numéro permettant d'identifier de manière unique les terminaux d'un téléphone mobile. Toute personne peut l'obtenir en composant le code : « *#06# » sur le clavier de son téléphone portable.

[32] L'adresse MAC est un identifiant stocké dans une carte réseau ou une interface réseau stockée dans l'ordinateur. Elle permet de se connecter au routeur d'un réseau. Art. 46*bis* CICr. Voy. J. Kerkhofs et P. Van Linthout, « L'article 46bis du Code d'instruction criminelle et l'obligation de motivation : de minimis non curat praetor ? », *T. Strafr.*, 2011/6, pp. 426-431.

[33] Ce seuil comprend un nombre important d'infractions. À titre illustratif, le vol simple est punissable d'une peine d'emprisonnement d'un mois à cinq ans et d'une peine d'amende de vingt-six à cinq cents euros (art. 463 C. pén.).

[34] Art. 46*bis,* § 1, dernier alinéa CICr. Ces données doivent être fournies « en temps réel » sous peine d'une peine d'amende de vingt-six euros à dix mille euros en cas de refus ou

Pour le repérage par contre, l'enquêteur devra solliciter l'autorisation d'un juge d'instruction. Cette mesure est en effet considérée comme plus intrusive puisqu'elle permet de procéder « au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées » ou à « la localisation de l'origine ou de la destination de communications électroniques »[35]. Autrement dit, le juge d'instruction est compétent pour demander l'isolement de certaines données d'appel, par exemple les différents numéros de téléphones composés ou reçus par un téléphone, leur durée, le moment de la prise de contact, etc.[36] Il peut également par ce biais localiser le signal émis par un appareil en fonctionnement sans qu'une communication ne soit émise ou reçue[37] et ainsi, géolocaliser une personne[38]. Dans certaines situations spécifiques de flagrant délit[39], ou en cas de harcèlement réalisé par le biais d'un réseau ou

d'absence de réaction. En outre, la loi prévoit une obligation à l'égard des tiers de « garder le secret » sanctionnée dans les mêmes conditions que celles prévues par l'article 458 du Code pénal garantissant le secret professionnel. Art. 46*bis,* §§ 2 et s., CICr.

[35] Art. 88*bis,* § 1, CICr.

[36] À noter que l'accès aux données de trafic et de localisation conservées par les opérateurs sur base de l'article 126 de la loi du 13 juin 2005, soit l'obligation de conservation des métadonnées est limité aux données stockées depuis six mois pour les infractions punies d'un à cinq ans d'emprisonnement, neuf mois lorsque l'infraction est de nature à emporter une peine de cinq ans ou plus, douze mois lorsqu'il est question de terrorisme (art. 88*bis,* § 2 CICr). Ces données doivent être fournies « en temps réel », obligation sanctionnée par une peine d'amende de vingt-six euros à dix mille euros en cas de refus ou d'absence de réaction. En outre, la loi prévoit une obligation à l'égard des tiers de « garder le secret » dont le non-respect est sanctionné dans les mêmes conditions que celles prévues par l'article 458 du Code pénal garantissant le secret professionnel (art. 88*bis,* § 4, CICr).

[37] Cass., 24 mai 2011, R.G. n° P.11.0909.N, *Pas.*, 2011.

[38] Cette mesure ne peut être ordonnée qu'en présence d'indices sérieux d'infractions de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde et pour autant que sa mise en œuvre s'avère nécessaire à la manifestation de la vérité. Le juge d'instruction indique les circonstances de fait de la cause qui justifient la mesure, son caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête dans une ordonnance motivée. Cette mesure doit être limitée dans le temps, deux mois maximums à dater de l'ordonnance postérieure ou antérieure sans préjudice de renouvellement (art. 88*bis*, §§ 1 et s., CICr).

[39] En cas de flagrant délit, le procureur du Roi peut également ordonner le repérage, pour les infractions visées à l'article 90*ter*, §§ 2, 3 et 4, CICr avec confirmation de la mesure dans les vingt-quatre heures par le juge d'instruction. En cas d'enquête relative à une infraction terroriste, prise d'otage, détention illégale ou extorsion, le procureur du Roi peut ordonner la mesure tant que la situation de flagrant délit perdure, sans qu'une confirmation par le juge d'instruction ne soit nécessaire. Uniquement concernant les infractions terroristes, le procureur du Roi peut ordonner le repérage des communications dans les septante-deux heures suivant la découverte de cette infraction, sans qu'une confirmation par le juge d'instruction ne soit nécessaire (art. 88*bis,* § 1, al. 6 et s., CICr).

d'un service de communications électroniques au sens de l'article 145, § 3 et § 3*bis*, de la loi du 13 juin 2005 relative aux communications électroniques[40], le procureur du Roi peut également ordonner un tel dispositif, sur demande du plaignant[41].

SECTION 3. – Les personnes soumises au secret professionnel

Pour certaines méthodes d'enquête, la loi prévoit des garanties supplémentaires à l'égard des avocats et des médecins en raison de la sensibilité des données qu'ils traitent et de l'importance du secret professionnel. Ainsi, le repérage des communications ne peut être exécutée que si le médecin ou l'avocat est lui-même soupçonné d'avoir commis une infraction ou d'y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une infraction utilisent ses moyens de communication électronique[42]. En outre, la mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins, selon le cas, en soit averti[43]. Dans le même sens, seul le juge d'instruction (et non le procureur du Roi) peut autoriser une observation systématique[44] ou un contrôle visuel discret[45] qui porte sur les locaux utilisés à des fins professionnelles ou la résidence d'un avocat ou d'un médecin ou une interception des communications[46], si celui-ci est lui-même soupçonné d'avoir commis une des infractions visées à l'article 90*ter* § 2 CICr[47], à savoir, le faux en informatique, la fraude informatique, les infrac-

[40] *M.B.*, 20 juin 2005.

[41] Art. 88*bis,* § 1, al. 9, CICr. On peut s'étonner d'un tel élargissement pour une infraction qui ne requiert pas la répétition du comportement incriminé, à la différence du harcèlement de droit commun (art. 442*bis* C. pén.). Dès lors, selon O. Leroux, il est réducteur de qualifier cette disposition de harcèlement (voy. O. Leroux (sous la direction de J.-F. Henrotte et F. Jongen), « Protection pénale des mineurs sur Internet : harcèlement, « Grooming » et cyberprédation », in *Pas de droit sans technologie*, Bruxelles, Larcier, 2015, p. 222).

[42] Art. 88*bis,* § 3, al. 1, CICr.

[43] Art. 88*bis,* § 3, al. 2, CICr.

[44] Art. 56*bis,* al. 2, CICr. L'article 47*sexies,* § 1, CICr définit l'observation par « une observation de plus de cinq jours consécutifs ou de plus de cinq jours non consécutifs répartis sur une période d'un mois, une observation dans le cadre de laquelle des moyens techniques sont utilisés, une observation revêtant un caractère international ou une observation exécutée par des unités spécialisées de la police fédérale ».

[45] Art. 89*ter* CICr.

[46] Art. 90*octies* CICr.

[47] Depuis l'adoption de la loi du 25 décembre 2016 et en dépit des réserves émises par la Commission de la protection de la vie privée, la liste des infractions a été considérablement

tions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et de leurs données dont le hacking, le harcèlement téléphonique, l'incitation à la débauche, l'embauche en vue de la débauche, le proxénétisme et la tenue de maison de débauche, l'enlèvement et le recel de mineur, l'extorsion et le vol à l'aide de violences ou de menaces commis avec ou sans circonstance aggravante, ou une infraction dans le cadre d'une organisation criminelle. La mesure peut également être ordonnée si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une de ces infractions utilisent ses locaux ou sa résidence. Il faut en outre que le bâtonnier ou le représentant de l'ordre provincial des médecins soit averti[48].

En revanche, la loi ne prévoit aucune protection spécifique à l'égard du médecin ou de l'avocat en cas de saisie de données informatiques ou de recherche dans un système informatique. Or, depuis l'adoption de la loi du 25 décembre 2016[49], tout officier de police judiciaire peut en effet effectuer une recherche dans un système informatique c'est-à-dire « lire, inspecter ou examiner des données »[50] pour autant qu'il agisse « sans but secret »[51] et après avoir saisi le support pour autant que l'appareil ne soit

élargies. Voy. Avis de la Commission de la protection de la vie privée, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 34.

[48] Art. 56*bis,* al. 3, CICr.

[49] Avant l'adoption de la loi du 25 décembre 2016, la procédure en vigueur prévoyait une distinction entre la saisie de données informatiques, relevant de la compétence du procureur du Roi, et la recherche ou l'extension de recherche dans un système, relevant de la compétence du juge d'instruction (art. 39*bis* CICr et 88*ter* CICr). Ce régime faisait l'objet de controverses, le Code d'instruction criminelle ne précisant pas si les enquêteurs pouvaient exploiter un système informatique sans disposer de l'autorisation d'un juge d'instruction. La question fut tranchée par la Cour de cassation dans un arrêt du 11 février 2015. La Cour dit pour droit que « l'exploitation de la mémoire d'un téléphone portable, dont les messages qui y sont stockés sous la forme d'un sms, est une mesure découlant de la saisie, laquelle peut être effectuée dans le cadre d'une information sans autres formalités que celles prévues pour cet acte d'enquête ». Cette jurisprudence fut entérinée par la loi du 25 décembre 2016 faisait fi de la nécessité de distinguer la « saisie » de données de la « recherche » dans un système dont la portée de l'ingérence diffère (Cass., 11 février 2015, R.G. n° P.14.1739.F., www.cass.be. Pour un commentaire d'arrêt voy. C. Forget, « Quelles garanties entourent la saisie de données informatiques et l'exploitation d'un système de données informatiques », *R.D.T.I.*, n° 61, décembre 2015, pp 79-90 ; C. Conings, « Het uitlezen van een gsm of een ander privaat IT-systeem: This is not America », noot onder Cass. 11 februari 2015, *R.W.,* 2015-2016, pp. 622-626).

[50] Rapport explicatif de la Convention de Budapest, § 191.

[51] Selon les travaux parlementaires, la distinction entre « secret » et « non secret » dépend premièrement, de l'intention des enquêteurs « de prendre connaissance des communications ou des données à l'insu des acteurs de ces communications ou à l'insu du propriétaire, du détenteur ou de l'utilisateur du système informatique » (Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 54). Deuxièmement, le caractère

pas verrouillé par un mot de passe ou si l'enquêteur dispose du code d'accès[52]. Dans l'hypothèse où le support n'est pas saisi mais pourrait l'être, par exemple si l'ordinateur est situé dans un cybercafé ou si l'enquête se déroule dans une banque, l'officier de police judiciaire doit requérir l'autorisation du procureur du Roi avant d'entamer une recherche[53]. À cette fin, l'enquêteur est tenu de couper les liaisons externes en activant, par exemple, le mode avion du téléphone[54]. Ainsi, des informations circulant par des services types WhatsApp, Viber, Hotmail, Gmail ou Facebook ne seront donc pas directement accessibles aux enquêteurs à moins d'être stockées et accessibles « hors connexion »[55]. Notons que si l'accès au système nécessite de faire usage de « fausses clés »[56], l'enquêteur devra obtenir l'autorisation du procureur du Roi dans le cadre d'une recherche ou du juge d'instruction dans le cadre d'une extension de recherche[57]. Si le système est chiffré, le procureur du Roi ou le juge d'instruction peut autoriser

non secret découle de l'obligation faites aux autorités de notifier « dans les plus brefs délais » au « responsable du système informatique » la recherche ou son extension, sauf si son identité ou son adresse ne peut « raisonnablement » être trouvée (art. 39*bis,* § 7, CICr).

[52] Art. 39*bis,* § 2, al. 1, et § 5, CICr. L'exploitation des données contenues dans un système informatique et la compétence des enquêteurs, est donc tributaire de la saisie d'un support et offre peu de garanties au justiciable en dépit d'une ingérence importante dans le droit au respect de la vie privée. À ce propos voy. C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique, vers un cadre (plus) strict ? », *op. cit.*, pp. 25-52.

[53] Art. 39*bis,* § 2, CICr.

[54] Art. 39*bis,* § 2, CICr.

[55] Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 17.

[56] Il s'agit de « tout moyen utilisé dans le but de contourner ou de craquer la sécurité d'un système informatique ou d'une partie de celui-ci afin d'obtenir l'accès – sous forme lisible – aux données contenues dans ce système ». Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 22.

[57] Le procureur du Roi peut autoriser l'extension de cette recherche vers d'autres systèmes ou parties de ceux-ci pour autant que l'enquêteur ne doive introduire aucun mot de passe, par exemple si celui-ci a été « retenu », peu importe que ce mot de passe soit identique ou différent à chaque fois (Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 20). L'extension de recherche doit par ailleurs être limitée aux parties auxquelles « les personnes autorisées à utiliser le système informatique » ont spécifiquement accès (art. 39*bis,* § 3, al. 3, CICr). L'autorisation doit être écrite, ou orale en cas d'urgence sous réserve de la confirmer dans les plus brefs délais (art. 39*bis*, § 3, al. 6, CICr). Elle doit être motivée et indiquer les raisons pour laquelle la mesure est, d'une part, nécessaire à la manifestation de la vérité et d'autre part, préciser en quoi l'exécution d'autres mesures serait disproportionnée ou s'il existe un risque de perdre certains éléments de preuve. Notons également que le juge d'instruction est compétent pour ordonner une recherche dans un système informatique ou une partie de celui-ci autres que celles visées par l'article 39*bis*, § 2 et § 3 CICr. (art. 39*bis,* § 4, CICr). Ainsi, par exemple, le magistrat instructeur pourra ordonner une recherche dans le compte Gmail d'un suspect sans qu'aucun appareil connecté à ce compte n'ait été saisi pour autant qu'il n'agisse pas « dans un but secret ».

« l'installation de dispositifs techniques dans les systèmes informatiques concernés en vue de décryptage et du décodage de données stockées, traitées ou transmises par ce système »[58].

L'exploitation des données contenues dans un système informatique et la compétence des enquêteurs sont donc tributaires de la saisie d'un support et offrent peu de garanties au justiciable en dépit d'une ingérence importante dans le droit au respect de la vie privée, ingérence d'autant plus importante pour les personnes soumises au secret professionnel[59]. En effet, un système informatique comprend des données relevant de la vie privée des personnes, par exemple, des données personnelles, des données professionnelles ou encore des données médicales. Il s'agit d'un espace virtuel pouvant être perçu par son utilisateur comme un lieu d'activité « au sein duquel un individu a le sentiment d'être dans l'intimité, en sécurité contre l'immixtion de personnes contre sa volonté, indépendamment de la durée et de l'intensité d'utilisation » à l'instar du domicile privé au sens de la jurisprudence de la Cour européenne des droits de l'homme[60]. L'intrusion dans ce système « privé » pourrait donc *a priori* être perçue pareillement à une mesure de perquisition au sens classique du terme[61].

Notre régime national semble peu conciliable avec la Convention de Budapest[62] d'autant que les enquêteurs ne sont pas tenus de disposer d'une autorisation préalable motivée du procureur du Roi ou du juge

[58] Art. 39*bis*, § 5, CICr.

[59] Dans l'arrêt *Niemietz*, la Cour européenne des droits de l'homme a expressément inclut les relations professionnelles dans le champ d'application du droit au respect de la vie privée. Elle précise en effet « n'y avoir aucune raison de principe de considérer cette matière de comprendre la notion de « vie privée » comme excluant les activités professionnelles ou commerciales : après tout, c'est dans leur travail que la majorité des gens ont beaucoup, voire le maximum d'occasions de resserrer leurs liens avec le monde extérieur ». Cour eur. D.H., *Niemietz c. la République fédérale d'Allemagne*, 16 décembre 1992, n° 13710/88, § 29.

[60] Voy. not. Cour eur. D.H., arrêt *Société Colas Est et autres c. France*, 16 avril 2002, n° 37971/97, § 41 ; Cour eur. D.H, arrêt *Van Rossem c. Belgique*, 9 décembre 2004, n° 41872/98.

[61] C. Meunier, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale a l'ère numérique », *Rev. dr. pén.*, 2001/7-8, pp. 663-664 ; T. Incalza, « Strafonderzoek in het digitale tijdperk: zoeking en inbeslagneming », *Jura Falc.*, 2010-2011/2, pp. 329-383.

[62] Selon ces dispositions, dans le cas d'une intrusion dans un système par des autorités en vue de saisir des données, la procédure applicable dans le contexte digital devrait s'aligner sur celle prévue « dans le cadre des pouvoirs traditionnels » de perquisition et de saisie. Or, le Code d'instruction criminelle plutôt que d'aligner la procédure relative à la recherche dans un système informatique sur la « perquisition », aligne celle-ci sur celle prévue en cas de saisie. Recommandation n° R(95)13 du Comité des Ministres aux États membres relative aux problèmes de procédure pénale liés à la technologie de l'information, 11 septembre 1995, § 2, et Rapport explicatif de la Convention sur la cybercriminalité, § 191.

d'instruction[63]. Cette autorisation permettrait de s'assurer de l'existence de soupçons raisonnables[64] à l'encontre de l'intéressé avant l'intervention des enquêteurs dans le système et ainsi éviter le risque de connaître une « *fishing expeditions* ». Ce type de mesure, autrement intitulée, saisie massive et indifférenciée » consiste en une fouille exercée dans l'espoir d'y trouver la preuve d'une infraction et entraine, selon la Cour européenne, une violation du droit au respect de la vie privée de la personne concernée[65]. La Cour autorise néanmoins une recherche effectuée de manière large c'est-à-dire sans cibler les dossiers à consulter, sur base de 35 mots-clés par exemple, pour autant que des garanties soient offertes à l'intéressé, en l'espèce, la présence de l'avocat mis en examen et d'un membre de l'ordre pendant la recherche dans le système ainsi que la rédaction d'un procès-verbal décrivant le déroulement des opérations[66]. Cette approche a

[63] Selon la Cour européenne des droits de l'homme, à l'instar d'une mesure de perquisition, la recherche dans un système informatique requiert en principe l'existence d'une autorisation préalable sauf exceptions. Ainsi, dans l'arrêt *Trabajo Rueda,* la Cour semble avoir implicitement reconnu qu'une recherche dans un système informatique requiert en principe une autorisation préalable sauf exceptions. Celle-ci précisa en effet en ces termes : « 35. La Cour constate que, en ce qui concerne l'accès au contenu d'un ordinateur personnel par la police, la jurisprudence du Tribunal constitutionnel a établi la règle de l'autorisation judiciaire préalable, condition exigée en tout état de cause par l'article 8 de la Convention (qui requiert la délivrance d'un mandat par un organe indépendant) lorsqu'une atteinte à la vie privée d'une personne est en jeu. La jurisprudence constitutionnelle espagnole permet toutefois, à titre exceptionnel, de passer outre une telle autorisation dans des situations d'urgence (« nécessité urgente ») pouvant faire l'objet d'un contrôle judiciaire postérieur ». Ce contrôle doit permettre de vérifier la réalité de l'urgence c'est-à-dire d'examiner l'existence de raisons pour lesquelles l'attente de cette autorisation risque d'entraver le bon déroulement de l'enquête. En l'espèce, les services de police avaient consulté les données contenues dans un ordinateur portable qui leur avait été remis. La Cour a considéré qu'il était difficile d'apprécier la réalité de l'urgence, la consultation de données informatiques visant les archives d'un système entre les mains des autorités et par ailleurs déconnecté d'Internet. Cour eur. D.H., *Trabajo Rueda c. Espagne*, 30 mai 2017, n° 32600/12, § 35.

[64] Comme le souligne le Juge Zupančič, « l'intrusion n'est donc justifiée qu'une fois le soupçon est déjà « raisonnable », c'est-à-dire lorsqu'il est très probable que le suspect a déjà enfreint la loi ». Selon ce dernier, le soupçon raisonnable devrait être « a priori », « concret », « spécifique » et « articulable » afin de permettre au juge de disposer au préalable d'informations réelles et pas seulement de l'intuition de l'autorité auteur de l'intrusion. Opinion concordante de Juge Zupančič, à laquelle se rallie le Juge De Gaetano, Cour eur. D.H., *Vinci construction et GMT Génie Civil et services c. France*, 2 avril 2014, n° 63629/10, §§ 78-79.

[65] Cour eur. D.H., *Sérvulo & Associados Advogados rl c. Portugal*, 3 septembre 2015, n° 27013/10.

[66] Cour eur. D.H., *Sérvulo & Associados Advogados rl c. Portugal*, 3 septembre 2015, n° 27013/10, § 103. Dans le même sens voy. Cour eur. D.H., *Wieser et Bicos Beteiligungen GmbH c. Autriche,* 16 octobre 2007, n° 74336/01.

également été retenue par la Cour de cassation dans le cadre d'une saisie opérée par l'autorité belge de la concurrence au sein d'une entreprise[67].

SECTION 4. – Les usagers de services de communications électroniques

La surveillance des communications fait l'objet de craintes sérieuses des usagers de services de communications électroniques qu'il s'agisse de l'obligation de rétention de métadonnées ou de l'interception du contenu des communications[68]. Examinons dès lors ces deux méthodes d'enquête.

[67] Cass., 22 janvier 2015, R.G. n° C.13.0532.F, www.cass.be. La Cour de cassation a considéré que « si, comme en l'occurrence, des données ont été copiées en masse, sans distinguer selon leur utilité en fonction des faits de la plainte, la méthodologie de sélection digitale conséquente doit permettre d'éviter que des documents qui n'ont aucun lien avec l'instruction fassent partie des fichiers de travail qui ont vocation à être transmis à l'équipe d'instruction ; L'utilisation de mots-clés adéquats en vue de la sélection, axes sur les faits directoires de la plainte, est dès lors essentielle, la pêche à l'infraction étant exclue ; 72. Dans le cas d'espèce, [le demandeur] a procède à la copie de centaines de milliers de mails et documents numériques (environ 760.000),dont il est apparu par la suite et provisoirement jusqu'à l'heure actuelle que, dans l'esprit [du demandeur], 38 p.c. peuvent revêtir un caractère utile pour l'instruction (environ 290.000 mails) ; Même après ces premières sélections, sur la base de 104 au lieu de 130 mots-clés, le nombre de données saisies retenues reste exceptionnellement élevé - rien que la lecture superficielle nécessiterait une dizaine de milliers d'heures de travail - et [la défenderesse] indique dans une annexe à ses conclusions que les mots-clés utilises jusqu'à présent n'ont pas évité d'inclure une quarantaine de sujets qui ne présentent aucun rapport avec le sujet de l'instruction ; Il peut raisonnablement en être déduit que les mots-clés utilises au stade actuel de la sélection ne répondent pas aux exigences de précision, d'adéquation et de proportionnalité et que, partant, leur application provoque un dépassement caractérise de l'ordre de perquisition (…) ».

[68] On peut noter qu'au niveau de la Cour européenne des droits de l'homme, de nombreuses plaintes ont été déposées notamment en raison du fait que cette dernière apprécie de manière large la qualité de « victime » facilitant ainsi l'introduction de recours « stratégique » d'associations de défense des droits de l'homme. En effet, ces mesures s'exerçant à l'insu des intéressés, la Cour ne se borne donc « pas à rechercher s'il existe une preuve directe de la mise en place d'une opération de surveillance, car pareille preuve est en général difficile – sinon impossible – à apporter » (Cour eur. D.H., *Kennedy c. Royaume-Uni*, 18 mai 2010, n° 26839/05, § 122). Selon cette dernière, la crainte ou menace de surveillance suffit en soi à restreindre la liberté des communications et constitue une ingérence au sens de l'article 8 de la CEDH (Cour eur. D.H., *Gerhard Klass e.a. c. Allemagne*, 6 septembre 1978 *Série A.*, vol. 28, § 41). La Cour estime dès lors qu'il se justifie de déroger à la règle selon laquelle les particuliers n'ont pas le droit de se plaindre d'une loi *in abstracto* afin de « s'assurer que le caractère secret de pareilles mesures ne conduise pas à ce qu'elles soient en pratique inattaquables et qu'elles échappent au contrôle des autorités nationales et de la Cour » (Cour eur. D.H., *Kennedy c. Royaume-Uni*, 18 mai 2010, n° 26839/05, § 124).

§ 1. L'obligation de rétention de données

L'obligation de rétention de données est une mesure controversée[69]. Elle consiste en la collecte et le stockage systématique et *a priori* de l'ensemble des « métadonnées » à savoir, les données traitées et générées lors d'une communication électronique à l'exception du contenu de celle-ci. Selon la Cour de justice de l'Union européenne, elle implique donc une ingérence « particulièrement grave » dans le droit au respect de la vie privée et à la protection des données à caractère personnel[70]. Actuellement, l'article 126 de la loi du 13 juin 2005 tel que modifié par la loi du 29 mai 2016[71] prévoit une obligation de rétention de données auprès des traditionnels opérateurs et fournisseurs de communications électroniques[72], tels Base, VOO ou encore Proximus[73]. Ces derniers sont tenus de stocker

[69] Pour une analyse voy. C. FORGET, « L'obligation de conservation des "métadonnnées" : la fin d'une longue saga juridique ? », *J.T.,* n° 6683, 2017, pp. 233-239.

[70] C.J.U.E., 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, C-293/12 et C-594/12.

[71] Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, *M.B.*, 18 juillet 2016.

[72] Plus précisément, il s'agit des « opérateurs fournissant des réseaux publics de communications électroniques ainsi [qu'aux] opérateurs fournissant un de ces services » mais aussi aux « fournisseurs au public de services de téléphonie, en ce compris par Internet, d'accès à l'Internet, de courrier électronique par Internet » .

[73] Les services « *over the top* » c'est-à-dire des services utilisant les réseaux de communications existants pour fournir des services de communications tels WhatsApp, Viber ou Facebook ne seraient pas concernés. À leur égard la question reste néanmoins controversée, d'autant plus que l'Union européenne projette de réglementer leurs activités afin de les soumettre aux obligations des opérateurs télécoms historiques. Voy. Proposition de Règlement du Parlement européen et du conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (Règlement « vie privée et communications électroniques »), Bruxelles, 10 janvier 2017, [COM(2017) 10 final], *J.O.,* 2017/0003(COD). Récemment, suite à un litige entre Skpe et l'Institut belge des services postaux et des télécommunications (IBPT), ce dernier ayant infligé une amende à la société américaine pour avoir refusé de se notifier comme opérateur pour le service SkypeOut, la Cour des marchés de Bruxelles a décidé de poser une question préjudicielle à la CJUE visant à déterminer si Skype doit être qualifié de services de communications électroniques (Bruxelles, arrêt du 7 février 2018 relatif au recours contre la décision du Conseil de l'IBPT du 30 mai 2016 relative à l'imposition d'une amende administrative à Skype Communications pour le non-respect de l'article 9, § 1er, de la loi du 13 juin 2005, disponible sur [http://www.ibpt.be/fr/operateurs/ibpt/litiges/annee-2018/arret-du-7-fevrier-2018-relatif-au-recours-contre-la-decision-du-conseil-de-libpt-du-30-mai-2016-relative-a-l-imposition-d-une-amende-administrative-a-skype-communications-pour-le-non-respect-de-larticle-9-1er-de-la-loi-du-13-juin-2005]).

pendant une période de douze mois les « métadonnées »[74] et de les transmettre « sans délai » sur demande des autorités compétentes[75].

La légalité de cette disposition semble toutefois être remise en cause depuis l'arrêt *Tele2* de la Cour de justice de l'Union européenne du 21 décembre 2016[76]. En effet, par ce biais, la Cour condamne sans ambages toute règlementation imposant la conservation « généralisée et indifférenciée » des données en raison de l'absence de différenciation, limitation ou exception en fonction de l'objectif poursuivi[77]. Dans la foulée, suite au recours en annulation introduit par l'Ordre des barreaux francophones et germanophone et les ASBL Liga voor Mensenrechten et Ligue des Droits de l'Homme, la Cour constitutionnelle a récemment décider de poser une question préjudicielle à la Cour de justice de l'Union européenne[78].

Quoiqu'il en soit, indépendamment d'une obligation légale, les tiers peuvent conserver certaines données à des fins de marketing ou de facturation par exemple[79]. De plus, elles peuvent être conservées à des fins de protection des données, la journalisation des données et l'enregistrement des logs par le responsable du traitement de données étant recommandé

[74] Art. 126, § 3, de la loi du 13 juin 2005 relatives aux communications électroniques, *M.B.*, 20 juin 2005.

[75] Art. 126, § 2, de la loi du 13 juin 2005. Il s'agit des autorités judiciaires conformément aux articles 46*bis* et 88*bis* du Code d'instruction criminelle, des services de renseignements et de sécurité, de tout officier de police judiciaire de l'IBPT dans le cadre d'une infraction prévue aux articles 114 (sécurité des données), 124 (atteinte à la confidentialité des communications) et 126 de la loi du 30 juin 2005, des services d'urgence offrant de l'aide sur place lorsqu'ils ne disposent pas des données d'identification de l'appelant, de l'officier de police judiciaire de la Cellule des personnes disparues de la Police Fédérale, du Service de médiation pour les télécommunications dans le cas d'utilisation malveillante des services de communications électroniques ou d'un réseau et des autorités prévues par la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques.

[76] C.J.U.E., 21 décembre 2016, *Tele2 Sverige AB/Post-och telestyrelsen et Secretary of State for the Home Department/Tom Watson e.a.*, aff. jointes C-203/15 et C-698/15 (ci-après arrêt *Tele2*).

[77] § 105 de l'arrêt *Tele2*.

[78] C. const., arrêt n° 96/2018 du 19 juillet 2018, n^{os} 6590, 6597, 6599 et 6601. La Cour constitutionnelle interroge la Cour de justice de l'Union européenne en vue de déterminer notamment si une règlementation nationale prévoyant une obligation de rétention des métadonnées est contraire au droit de l'Union européenne sans préjudice des garanties qu'elle prévoit.

[79] Les opérateurs par exemple, peuvent stocker des métadonnées à des fins à des fins de marketing et de facturation en vertu des articles 122 et 123 de la loi du 13 juin 2005. Ces articles transposent les articles 5 et 6 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, *J.O.C.E.*, L 201/37, 31 juillet 2002, pp. 0037-0047.

en vue de favoriser la sécurité informatique[80]. Ces données peuvent être requises par les enquêteurs sur base des articles 46*bis* et 88*bis* du Code d'instruction criminelle règlementant respectivement l'identification et le repérage que nous avons exposé *supra*.

§ 2. L'interception du contenu des communications

Dans le domaine des mesures de surveillance secrète[81], la Cour européenne des droits de l'homme tient compte des critères suivants : « la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée d'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties, et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements »[82].

En droit belge, l'interception, la prise de connaissance, l'exploration, l'enregistrement de communications non accessibles au public ou de données informatiques « en secret »[83] relève de la compétence du juge d'instruction[84]. Pour accéder au système, il peut ordonner l'utilisation de

[80] À ce propos voy. par exemple : Groupe 29, Lettre du 5 juillet 2018 adressée à l'Internet Corporation for Assigned Names and Numbers (ICANN), p. 5 disponible sur [https://edpb.europa.eu/sites/edpb/files/files/news/icann_letter_en.pdf]

[81] La Cour européenne des droits de l'homme apprécie le caractère prévisible d'une telle disposition en tenant compte du fait qu'elle s'exerce en secret. Selon la Cour, la prévisibilité « ne saurait signifier qu'un individu doit se trouver à même d'escompter quand les autorités sont susceptibles d'intercepter ses communications de manière qu'il puisse adapter sa conduite en conséquence ». Toutefois, la base légale applicable doit « prévoir en termes suffisamment clairs et détaillés les circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrètes » et ceci, « d'autant que les procédés techniques utilisables ne cessent de se perfectionner » (Cour eur. D.H., *Weber et Saravia c. Allemagne*, 19 mai 2010, n° 26839/05, § 93).

[82] Cour eur. D.H. (GC), *Roman Zakharov c. Russie*, 4 décembre 2015, n° 47143/06, § 231. Pour une analyse plus approfondie voy. C. FORGET, « Procédure et méthodes d'investigation sur Internet », in *L'Europe des droits de l'Homme à l'heure d'Internet*, Bruxelles, Bruylant, *à paraître.*

[83] En ce sens, il se distingue de l'article 39*bis,* § 4, CICr, permettant au juge d'instruction d'effectuer une recherche en réseau dans un système informatique sous réserve de certaines conditions.

[84] Art. 90*ter* et s. CICr. À noter que cette méthode ne peut excéder un mois à dater de la première autorisation sans préjudice de renouvellement avec une période maximale de six mois, sauf en cas de retard dû à sa préparation technique. Elle ne peut être ordonnée que de manière exceptionnelle, lorsque les nécessités de l'instruction l'exigent, en présence d'indices sérieux d'une infraction visée par l'article 90*ter*, § 2, CICr, à savoir, le faux en informatique, la fraude informatique, les infractions contre la confidentialité, l'intégrité et

fausses clés[85], la suppression de manière temporaire des protections du système informatique ou en encore l'installation de dispositifs techniques dans les systèmes informatiques concernés en vue du décryptage et du décodage de données stockées, traitées ou transmises par ce système[86]. Ainsi libellée, la disposition permet par exemple, aux enquêteurs de placer un logiciel espion sur l'ordinateur d'une personne en vue d'exploiter le contenu du disque dur ou d'intercepter une conversation et d'en prendre copie[87]. Ce type de programme peut être installé à l'insu de l'utilisateur par exemple, par le biais d'une mise à jour du système d'exploitation ou en envoyant un message électronique comprenant une pièce jointe qui, une fois ouverte, entraîne l'installation automatique[88]. Les enquêteurs pourront par ce biais accéder aux communications véhiculées par des dispositifs « VoIP »[89] soit par exemple, WhatsApp, Viber ou Skype lesquels ont la particularité d'être souvent chiffrés et inaccessibles. Outre l'interception des communications, la faculté de ces logiciels est infinie : certains peuvent surveiller un ordinateur et intercepter l'ensemble des données informatiques par exemple, les entrées clavier, les mots de passe, d'autres interceptent les échanges de flux de données circulant via l'appareil et par Internet[90]. La mesure peut donc s'avérer particulièrement intrusive pour la vie privée des personnes concernées. L'article 90*novies* CICr prévoit par ailleurs, une obligation d'informer toute personne ayant fait l'objet d'une

---

la disponibilité des systèmes informatiques et de leurs données dont le hacking, l'infraction visée à l'article 145, §§ 3 et 3*bis*, de la loi du 13 juin 2005 relative aux communications électroniques tel le harcèlement téléphonique, l'incitation à la débauche, l'embauche en vue de la débauche, le proxénétisme et la tenue de maison de débauche, l'enlèvement et le recel de mineur, l'extorsion et le vol à l'aide de violences ou de menaces commis avec ou sans circonstance aggravante. De plus, la loi exige le respect du critère de subsidiarité dans la mesure où un tel dispositif ne peut être imposé que si d'autres moyens d'investigation ne paraissent pas suffire à la manifestation de la vérité. Celle-ci ne peut être exécutée à des fins exploratoires ou dans le cadre d'une mini-instruction et reste donc de la compétence unique du juge d'instruction, sauf cas particulier du flagrant délit dans le cadre d'infractions terroristes par exemple, où le procureur du Roi disposera de compétences importantes.

[85] Sur la notion de « fausses clés » voy. *supra* : Le déverrouillage du système informatique.

[86] Art. 90*ter,* § 1, al. 3, CICr.

[87] Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 57.

[88] M. Zwolinska, « Sécurité et les libertés fondamentales des communications électroniques en droit français, européen et international », thèse sous la direction de Louis Balmond, Nice, 2015, p. 300.

[89] Ces services permettent de communiquer via le réseau Internet en faisant usage du protocole TCP/IP.

[90] M. Zwolinska, « Sécurité et les libertés fondamentales des communications électroniques en droit français, européen et international », *op. cit.*, p. 300.

mesure visée par l'article 90*ter* CICr, de la nature de ladite mesure et des dates auxquelles elle a été exécutée[91].

En dépit des réserves émises par la Commission de la protection de la vie privée, la loi du 25 décembre 2016 a élargi de manière importante la liste des infractions visées par l'article 90*ter*, § 2, CICr en incluant par exemple, l'attentat à la pudeur, le viol, le grooming, le vol à l'aide de violence ou menaces, le trafic de stupéfiants, l'incendie et la tentative d'incendie, le hacking, le faux informatique, les infractions relatives au secret des communications, sans qu'un débat parlementaire approfondi n'ait eu lieu[92]. De plus, on peut s'interroger sur la compatibilité d'un tel dispositif avec la Convention de Budapest exigeant de limiter ce type de méthode aux enquêtes relatives à « un éventail d'infractions graves à définir en droit interne »[93].

SECTION 5. – L'intérêt légitime du tiers

Les mesures de cryptage permettent d'assurer la protection des données à caractère personnel[94] et en ce sens, contribuent à protéger le droit au respect de la vie privée[95]. Afin de permettre une recherche dans un système informatique ou une saisie de données informatiques, les importateurs

[91] Cette notification doit intervenir au plus tard quinze jours après le moment où la décision sur le règlement de la procédure est devenue définitive ou après que la personne concernée ait été citée, sauf si son identité ou son adresse ne peut « raisonnablement » être trouvée.

[92] Avis de la Commission de la protection de la vie privée, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 34.

[93] Art. 21, § 1, de la Convention de Budapest.

[94] Différents instrumentions internationaux préconisent le chiffrement de données en vue d'assurer la sécurité des flux et la protection des données à caractère personnel. L'article 31, § 1, du Règlement général sur la protection des données liste certaines mesures permettant de garantir un niveau de sécurité informatique adapté dont la première est « le chiffrement des données à caractère personnel ». De même, une Recommandation du Comité des Ministres du Conseil de l'Europe préconise l'application de mesures de cryptage « de bout en bout » afin d'éviter l'accès illite aux données par des tiers. Voy. Recommandation CM/Rec (2014)6 du Comité des Ministres aux États membres sur un Guides des droits de l'homme pour les utilisateurs d'internet, adoptée par le Comité des Ministres le 16 avril 2014 ; dans le même sens, l'Assemblée parlementaire du Conseil de l'Europe affirme qu'un « cryptage généralisé destiné à renforcer le respect de la vie privée reste la riposte la plus efficace pour permettre aux citoyens de protéger leurs données », voy. Rapport de la commission des questions juridiques et des droits de l'homme de l'Assemblée parlementaire du Conseil de l'Europe, rapporteur : M. Pieter Omtzigt, Doc. 13734, 18 mars 2015, pt 119.

[95] Ce lien de dépendance a été illustré dans l'arrêt *I. c. Finlande* où la Cour européenne des droits de l'homme estima que le défaut de garanties relatives à la sécurisation des

de distributeurs d'ordinateurs ou de logiciels, les "*trusted third parties*", les fournisseurs de service, d'opérateurs, les ingénieurs d'entreprise ayant élaboré une configuration informatique spécifique, les spécialistes de la sécurité, etc.[96], peuvent être tenus, sur base d'une ordonnance motivée du juge d'instruction, de prêter leurs concours en fournissant certaines informations[97]. De plus, le juge d'instruction peut ordonner à « toute personne appropriée » de mettre ledit système en fonctionnement et de procéder à une recherche ou à une saisie de données informatiques et à fournir certaines données dans la forme qu'il aura demandé[98]. Le défaut de collaboration est passible de sanctions pénales[99].

À la différence de l'obligation « d'information », l'obligation « d'action » est un « engagement à fournir des efforts », le législateur considérant qu'on ne peut attendre d'une personne qu'elle déploie des moyens qu'elle est incapable de fournir[100]. La loi prévoit donc expressément que les personnes sont tenues de donner suite à l'ordonnance du juge d'instruction « dans la mesure de leurs moyens »[101]. En pratique cependant, l'enquêteur sera tenté de détourner cette limite en imposant le concours de tiers sur une autre base légale telle que l'interception des communications visée par l'article 90*quater* CICr. L'affaire rendue récemment par la cour d'appel d'Anvers permet d'illustrer notre propos puisqu'une ordonnance du juge d'instruction prise sur base des articles 88*bis* CICr et 90*quater* CICr imposait à Skype de collaborer en vue de permettre l'interception

données contre des usages non-autorisés constitue une violation de l'obligation positive d'assurer le respect du droit à la vie privée consacré à l'article 8 de la CEDH. Cour eur. D.H., *I. c. Finlande*, 17 juillet 2008, n° 20511/03.

[96] *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 50.

[97] Cette ordonnance peut être prise de manière large à l'égard de « quiconque dont on présume » qu'il a une connaissance particulière du système informatique visé relatives à son fonctionnement ou la manière d'y accéder, par exemple les clés de chiffrement ou les mots de passe. Voy. art. 88*quater,* § 1, CICr.

[98] Art. 88*quater*, § 2, CICr.

[99] Le défaut de collaboration est passible de sanctions pénales à savoir, une peine d'emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à vingt mille euros ou d'une de ces peines seulement. Cette sanction peut être portée d'un à cinq ans avec une peine d'amende de cinq cents euros à cinquante mille euros dans le cas où la collaboration aurait eu pour effet d'empêcher la commission d'un crime ou d'un délit ou d'en limiter les effets. En outre, la loi prévoit une obligation à l'égard des tiers de « garder le secret » sanctionnée dans les mêmes conditions que celles prévues par l'article 458 du Code pénal garantissant le secret professionnel. On précisera que la mesure ne peut porter atteinte au droit au silence et aux règles de droit commun relatives aux personnes tenues au secret professionnel (art. 88*quater*, §§ 3-4, CICr).

[100] *Doc. parl.*, Ch. repr., 1999-2000, n° 0213/001, p. 27.

[101] Art. 88*quater,* § 2, CICr.

des données de communications électroniques[102]. L'entreprise invoquait l'impossibilité matérielle de prêter son concours en raison du chiffrement des données depuis le destinateur et le déchiffrement une fois chez le destinataire. Or, l'article 90*quater* CICr ne souffre d'aucune dérogation à l'obligation de collaboration. Dès lors, selon la cour d'appel, en créant ses services, Skype aurait dû tenir compte des obligations de collaboration découlant du droit national belge. Ce faisant, la cour déduit de l'article 90*quater* CICr une obligation positive de collaboration potentielle à charge des tiers dès la conception d'application. Cette interprétation peut sembler entrer en résonnance avec les concepts de « *privacy by design* » ou de « *privacy by default* » qui imposent au responsable du traitement de prendre en considération, dès la conception, la nécessité de mettre en œuvre des mesures techniques et organisationnelles appropriées[103]. Cependant, la question mérite d'être posée quant à savoir si ces approches vont jusqu'à leur imposer des obligations de « *collaboration by design* » avec les autorités policières et judiciaires. Rappelons enfin que, selon la Convention de Budapest, les autorités répressives se heurtant à des données chiffrées[104] peuvent imposer la collaboration de tiers afin d'obtenir les données en sa possession ou sous son contrôle[105] en « texte clair »[106] c'est-à-dire déchiffrées. Considérant qu'il s'agit d'une méthode d'enquête, elle exige le respect du critère de proportionnalité mais aussi de prendre en considération l'intérêt légitime de tiers[107].

---

[102] Anvers (4e ch.) n° 2016/CO/1006, 15 novembre 2017.

[103] Art. 25 du RGPD.

[104] Europol affirme que le chiffrement des données ralentit considérablement la poursuite des enquêtes pénales. Europol, « The Internet Organised Crime Threat Assessment (IOCTA) 2015 », 30 septembre 2015, pp. 67 et s.

[105] L'expression « en sa possession » ou « sous son contrôle » fait référence d'une part, à la possession matérielle des données et d'autre part, à des situations dans lesquelles l'intéressé ne possède pas matériellement les données à produire mais peut en contrôler librement la production, par exemple si les données sont stockées sur un cloud qu'il met librement à disposition. Le rapport explicatif précise toutefois qu'un accès aux données par une liaison du réseau ne constitue pas nécessairement un « contrôle » au sens de la présente disposition. Rapport explicatif de la Convention sur la cybercriminalité, Conseil de l'Europe, Budapest, 23 novembre 2001, § 173.

[106] Rapport explicatif de la Convention sur la cybercriminalité, Conseil de l'Europe, Budapest, 23 novembre 2001, § 176.

[107] Art. 18, § 2, de la Convention de Budapest. À titre illustratif, l'affaire *Apple* défraya la chronique en raison du refus de l'entreprise d'obtempérer à une injonction du FBI lui ordonnant de déchiffrer le téléphone portable d'un des auteurs de la tuerie de San Bernardino. Apple refusa d'agir invoquant le risque de mettre à mal la sécurité informatique de ses services d'autant qu'outre le déblocage du téléphone, le FBI souhaitait qu'Apple élabore une nouvelle version du système d'exploitation afin de faciliter de manière générale l'accès des autorités aux données stockées sur ses appareils, indépendamment de celui visé dans le

SECTION 6. – L'obligation de collaboration du suspect

Le droit de ne pas contribuer à sa propre incrimination et le droit de garder le silence sont des normes internationales généralement reconnues qui sont au cœur de la notion de procès équitable[108]. Le droit au silence n'est pas expressément visé par l'article 6, § 3, de la Convention mais a progressivement été défini par la jurisprudence[109]. Ainsi, selon la Cour européenne des droits de l'homme, « le droit de ne pas contribuer à propre incrimination présuppose que, dans une affaire pénale, l'accusation cherche à fonder son argumentation sans recourir à des éléments de preuve obtenus par la contrainte ou les pressions, au mépris de la volonté de l'accusé. En ce sens, ce droit est étroitement lié au principe de la présomption d'innocence »[110]. En conséquence, le Code d'instruction criminelle prévoit expressément que « l'obligation d'agir » dans le système informatique, prise sur base d'une ordonnance du juge d'instruction, ne peut être adressée à un inculpé et aux personnes visées par l'article 156 CICr[111] à savoir, les ascendants ou descendants de la personne prévenue ainsi que ses proches.

Par contre, la loi ne précise pas si l'ordonnance relative à l'obligation de fournir certaines informations peut être adressée à un suspect[112]. Dans un jugement du 17 novembre 2014, le tribunal correctionnel de Termonde a rappelé qu'aucun suspect ne peut être obligé de collaborer activement avec les autorités poursuivantes. Il estima qu'en ordonnant aux prévenus de rendre accessibles les supports de données, ils avaient été contraints, moyennant une prestation intellectuelle propre, de contribuer activement à l'administration de la preuve de sorte que les éléments de preuve fournis par les supports de données cryptées étaient frappés de nullité[113]. Cette approche fut confirmée par la cour d'appel de Gand[114]. En effet, le droit au silence ne couvre pas uniquement le droit de se taire mais englobe

---

cadre de l'enquête. *In fine,* le FBI trouva une faille et accéda aux données contenues sur le téléphone sans la collaboration de la multinationale et *a fortiori,* sans devoir approfondir la question de l'intérêt légitime d'un tiers à la procédure.

[108] Cour eur. D.H., *Brusco c. France*, n° 1466/07 ; CEDH, 14 octobre 2010, § 44.

[109] Voy. entre autres, Cour eur. D.H., 25 février 1993, *Funke c. France*, § 44 ; Cour eur. D.H., *Saunders* c. *Royaume-Uni*, n° 19187/91 ; CEDH, 1996-VI, § 65 ; Cour eur. D.H., *John Murray* c. *Royaume-Uni*, n° 18731/91, §§ 45, 47 et 50 ; Cour eur. D.H., *Condron* c. *Royaume-Uni*, n° 35718/97 ; Cour eur. D.H., 2 mai 2000, *Heaney et McGuiness* c. *Irlande*, n° 34720/97.

[110] H.-D. Bosly, D. Vandermeersch et M.-A. Beernaert, *Droit de la procédure pénale*, 6e éd., Bruxelles, la Charte, 2010, pp. 28 et 30 spéc. les notes nos 103 et 115.

[111] Art. 88*quater,* § 2, al. 2, CICr.

[112] Art. 88*quater,* § 1, CICr.

[113] Corr. Termonde, 17 novembre 2014, *T. Strafr.*, 2016/3, pp. 255-260.

[114] Gand 23 juin 2015, *NjW,* 2016, liv. 336, p. 134, note C. Conings.

également le droit de ne pas devoir fournir des informations susceptibles d'affecter substantiellement la position de l'accusé ou de favoriser une incrimination.

Récemment toutefois, la cour d'appel d'Anvers, chambre des mises en accusation, a considéré que l'ordonnance d'un juge d'instruction imposant à un inculpé de dévoiler le code pin de son téléphone portable sous peine de sanctions pénales, n'était pas incompatible avec les exigences du droit à un procès équitable[115]. Cette dernière considère en effet que la clé de chiffrement n'est pas en soi incriminante mais ce sont les données stockées dans le système informatique qui peuvent l'être. De plus, le juge fait mention du fait que la loi ne prévoit pas une telle dérogation et ce conformément à l'arrêt *Saunders* de la Cour européenne des droits de l'homme, arrêt auquel s'est par ailleurs référé le législateur dans les travaux préparatoires[116]. Dans cette décision, la juridiction de Strasbourg effectue une distinction entre les données recueillies « au mépris de la volonté du suspect » et les données que l'on peut obtenir de l'accusé en recourant à des pouvoirs coercitifs mais « qui existent indépendamment de sa volonté » telles des documents recueillis sur base d'un mandat, des empreintes ADN, haleine, sang, urine[117]. Selon la Cour européenne, cette dernière catégorie n'entre pas dans le champ d'application du droit au silence[118]. En tout état de cause, la chambre des mises en accusation estime que même en faisant application du droit au silence, elle rappelle qu'il ne s'agit pas d'un droit absolu. En application du principe de proportionnalité, elle estime que l'ingérence ne peut être qualifiée de grave et qu'elle se justifie dans l'intérêt public[119].

---

[115] Anvers, 21 décembre 2017, chambre des mises en accusation, K/2895/2017, inédit. Dans la foulée, la cour d'appel de Gand (chambre des mises en accusation) a rendu une décision similaire estimant qu'il s'agit d'une obligation de collaboration passive. Voy. Gand, 16 janvier 2018, KI2018/22/2, inédit.

[116] *Doc. parl.*, Ch. repr., 1999-2000, n° 50-0213/001, p. 27.

[117] Cour eur. D.H., *Saunders c. Royaume-Uni*, 17 décembre 1996, n° 1187/91, § 69.

[118] Cour eur. D.H., *Saunders c. Royaume-Uni*, 17 décembre 1996, n° 1187/91, § 69.

[119] La validité de cette distinction a été critiquée dans une opinion dissidente. Il y était relevé que : « Pour quelle raison un suspect aurait-il le droit de ne pas subir de pressions pour l'obliger à faire des déclarations l'incriminant, mais pourrait-il être forcé à coopérer pour fournir des données à charge ? La nouvelle raison d'être adoptée par la Cour ne justifie pas cette distinction puisque dans les deux cas, la volonté du suspect n'est pas respectée : en effet, il est contraint de participer à sa propre condamnation. De plus, le critère utilisé pour établir la distinction n'est pas sans poser de problème. Peut-on vraiment dire que le contenu d'un ballon d'alcootest dans lequel une personne soupçonnée de conduite en état d'ivresse a été contrainte de souffler a une existence indépendante de la volonté du suspect ? Que dire d'un code PIN ou de la clé d'un système de chiffrement, enfouis dans la mémoire du suspect ? ». Cour eur. D.H., *Saunders c. Royaume-Uni*, 17 décembre 1996, n° 1187/91, opinion dissidente du juge Martens à laquelle le juge Kuris déclare se rallier, I. C.12.

L'analyse critique de cet arrêt dépasserait le cadre de cette contribution. Soulignons toutefois que l'on pourrait soutenir qu'à la différence de documents fiscaux tenus en vertu d'une obligation légale et saisissables dans le cadre d'une perquisition par exemple, un mot de passe peut être créé sur initiative de son auteur et devrait donc en ce cas, être couvert par le droit au silence[120]. En revanche, dans certaines situations, un mot de passe consiste en un système d'authentification par empreinte digitale ou encore par reconnaissance faciale. En ce cas, la collaboration pourrait être due considérant que les données existent indépendamment de la volonté de l'auteur. Insistons toutefois sur le fait que dans ce dernier cas, si les autorités doivent contraindre physiquement le suspect à collaborer, le recours à des pouvoirs coercitifs ne peut se faire à n'importe quel prix. Pour examiner la compatibilité d'un tel dispositif avec le droit au silence, la Cour européenne des droits de l'homme examine par exemple tour à tour les facteurs suivants : la nature et le degré de la coercition employée pour l'obtention des éléments de preuve ; le poids de l'intérêt public à la poursuite de l'infraction en question et à la sanction de son auteur ; l'existence de garanties appropriées dans la procédure et l'utilisation faite des éléments ainsi obtenus[121].

En outre, concernant les sanctions pénales, on peut se demander quels seraient les conséquences d'un défaut de collaboration en cas d'oubli du mot de passe ou d'absence de conservation de la clé de chiffrement laquelle n'est imposée par aucune obligation légale. En effet, comme précisé *supra*, si, le Code d'instruction criminelle précise que les personnes sont tenues de donner suite à l'ordonnance relative à l'obligation d'agir

[120] Cour eur. D.H., *Funke c. France*, 25 février 1993, n° 110588/83. Notons qu'en France, une telle obligation a été validée par le Conseil constitutionnel considérant que « Les dispositions critiquées n'imposent à la personne suspectée d'avoir commis une infraction, en utilisant un moyen de cryptologie, de délivrer ou de mettre en œuvre la convention secrète de déchiffrement que s'il est établi qu'elle en a connaissance. Elles n'ont pas pour objet d'obtenir des aveux de sa part et n'emportent ni reconnaissance ni présomption de culpabilité mais permettent seulement le déchiffrement des données cryptées. En outre, l'enquête ou l'instruction doivent avoir permis d'identifier l'existence des données traitées par le moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit. Enfin, ces données, déjà fixées sur un support, existent indépendamment de la volonté de la personne suspectée ». Voy. Décision n° 2018-696 du Conseil Constitutionnel, QPC du 30 mars 2018 *JORF* n° 0076 du 31 mars 2018 texte n° 111 ECLI:FR:CC:2018:2018.696.QPC.

[121] Cour eur. D.H., *Jalloh c. Allemagne,* 11 juillet 2006, n° 54810/00, § 117.

« dans la mesure de leurs moyens »[122], l'obligation d'information ne souffre par contre aucune dérogation[123].

Conclusion

Les méthodes d'enquête pénales dans un contexte informatique sont susceptibles d'impliquer différentes catégories de personnes considérées comme « vulnérables » en raison du risque d'ingérence illicite ou arbitraire dans leurs droits et libertés fondamentales. Indépendamment de leur statut dans le cadre du procès pénal, elles bénéficient de protections particulières limitant la latitude des autorités répressives.

Dès lors, comme exposé dans le cadre de cette contribution, le Code d'instruction criminelle offre des garanties spécifiques à l'hébergeur mais aussi aux personnes actives sur Internet ou encore aux utilisateurs de communications électroniques.

On peut par contre regretter que les personnes soumises au secret professionnel ne bénéficient pas d'un cadre légal plus strict dans le cadre de la recherche dans un système informatique « sans but secret » et la saisie de données informatiques, mesures pouvant s'avérer particulièrement invasives dans le droit au respect de la vie privée. En outre, on peut espérer que la jurisprudence sera amenée à préciser les contours de l'obligation de collaboration des tiers mais aussi du suspect contraint de fournir certaines informations.

En tout état de cause, rappelons que ces garanties sont d'autant plus essentielles que l'article 32 du Titre préliminaire du Code de procédure pénale mentionné dans les travaux parlementaires de la loi du

[122] Art. 88*quater,* § 2, CICr.

[123] En ce sens, la directive relative à la présomption d'innocence et au droit d'assister à son procès dans le cadre des procédures pénales précise « L'exercice du droit de ne pas s'incriminer soi-même ne devrait pas empêcher les autorités compétentes de réunir les preuves que l'on peut obtenir légalement du suspect ou de la personne poursuivie en recourant à des pouvoirs de contrainte licites et qui existent indépendamment de la volonté du suspect ou de la personne poursuivie, tels que des documents recueillis en vertu d'un mandat, des documents pour lesquels est prévue une obligation légale de conservation et de production sur demande, les échantillons d'air expiré, de sang et d'urine ainsi que les tissus corporels en vue d'une analyse de l'ADN ». Cette directive requiert donc *a priori* un lien entre la production sur demande et l'obligation de conservation de données ce qui n'est pas le cas pour un mot de passe. Considérant 29 de la directive 2016/343/UE du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales, *O.J.*, L 65, 11 mars 2016, pp. 1-11.

25 décembre 2016 en tant que garantie en cas de violation de droits fondamentaux ne paraît pas pertinent[124]. Celui-ci permet la « mise à l'écart » des preuves obtenues irrégulièrement en cas d'atteinte au procès équitable[125]. Il ne saurait donc réparer les manquements en cas d'ingérence illicite et arbitraire dans le droit au respect de la vie privée. Nous verrons si la jurisprudence permettra de clarifier certains points et si les garanties fournies au justiciable seront en pratique effectives et non théoriques et illusoires.

[124] Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 54-1966/001, p. 61.

[125] Pour une analyse détaillée voy. F. LUGENTZ, *La preuve en matière pénale*, Limal, Anthemis, 2017.